UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

RON GILBERT, on behalf of himself and on behalf of all others similarly situated, Plaintiff, v. AFTRA RETIREMENT FUND and THE SAG-AFTRA HEALTH PLAN, Defendants.	Case No. _____ **COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff Ron Gilbert ("Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Defendants AFTRA Retirement Fund ("AFTRA Retirement") and The SAG-AFTRA Health Plan ("SAG-AFTRA Health") ("Defendants") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters as follows:

NATURE OF THE ACTION

1. Plaintiff and other members of the putative class ("Class Members") are individuals whose Personally Identifiable Information ("PII") -- including their addresses, dates of birth, driver's license numbers, state identification numbers, financial or banking information, health insurance numbers, Social Security numbers, and email addresses -- were compromised due to Defendants' failure to implement and maintain reasonable safeguards to protect such information.

2. This class action seeks to redress Defendants' unlawful and negligent disclosure of over 57,000 individuals' PII in a massive data breach on or around October 28, 2019 ("Data Breach" or "Breach"), in violation of state statute and common law. On that date, and possibly on

others, Defendants' inadequate security measures allowed unauthorized individuals to access and obtain the AFTRA Retirement's computer network that contained the PII of Plaintiff and other individuals.

3. Defendants have acknowledged that a cybersecurity incident occurred, resulting in possible unauthorized access to AFTRA Retirement members' data.

4. Defendants only announced the Data Breach some four months later, on February 25, 2020, in a press release entitled "AFTRA Retirement Fund – Notice of Data Privacy Event" (the "Press Release").[1] During that period, Plaintiff and Class Members were wholly unaware that their critical PII had been compromised.

5. According to the Press Release, the Data Breach "may have impacted the security of personal information of certain current and former plan members of SAG-AFTRA Health Plan," indicating that Class Members' Protected Health Information ("PHI") entrusted to SAG-AFTRA Health might also have been compromised.

6. Defendants could have prevented this Data Breach.

7. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to: (i) take adequate and reasonable measures to ensure AFTRA Retirement's data systems were protected; (ii) disclose to its members the material fact that it did not have adequate security practices to safeguard PII; (iii) take available steps to prevent and stop the breach from ever happening; and (iv) monitor and detect the breach on a timely basis.

8. As a direct result of Defendants' negligent failure to protect the PII with which it was entrusted, Plaintiff and Class Members will bear an immediate and heightened risk of all

[1] https://www.prnewswire.com/news-releases/aftra-retirement-fund---notice-of-data-privacy-event-301011163.html

manners of identity theft. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of the Data Breach, include the:

a. unauthorized use of Class Members' PII and/or PHI;

b. damages arising from the inability to use their PII and/or PHI;

c. theft of their personal and financial information;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and/or PHI being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class Members' information on the Internet black market;

h. damages to and diminution in value of their PII and/or PHI entrusted to AFTRA Retirement for the sole purpose of remaining retirement plan members; and

i. the loss of Plaintiff's and Class Members' privacy.

9. Further, Plaintiff and Class Members retain a significant interest in ensuring that their PII and/or PHI, which, while stolen, remains in the possession of Defendants, is protected from further breaches.

10. Plaintiff incurred, and will continue to incur, damages in the form of, *inter alia*, loss of privacy and/or the additional damages set forth in detail below.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and one Defendant are citizens of different states. The proposed Nationwide Class and California Sub-class each include well over 100 members.

12. This Court has jurisdiction over Defendants because Defendant AFTRA Retirement is headquartered in New York. Additionally, Defendant SAG-AFTRA Health, whose member information was also compromised in the same Data Breach, intentionally avails itself of this jurisdiction by: (1) maintaining an office in New York; and (2) marketing and offering its health plan services to thousands of SAG-AFTRA members in New York.

PARTIES

13. Plaintiff Ron Gilbert is a resident of California and is a member of the SAG-AFTRA Health Plan and the AFTRA Retirement Fund. On or about February 25, 2020 Mr. Gilbert received notice from Defendants informing him that his PII may have been breached in October 2019 -- including, potentially, his "Name, SSN, AFTRA Number, Date of Birth, Date of Death, Address, Past Information about: eligibility, dependent(s), claims, earnings, contributions, and

beneficiaries." If Mr. Gilbert had known that Defendants would not adequately protect his PII, he would not have allowed Defendants access to this sensitive and private information.

14. Defendant AFTRA Retirement Fund is a retirement fund with its principal place of business at 261 Madison Avenue, 7th floor, New York, NY 10016-2309. AFTRA Retirement claims to have provided retirement benefits to performers for nearly 60 years. According to AFTRA Retirement's website, "AFTRA Retirement Fund is a separate legal entity from SAG-AFTRA, the union. The AFTRA Retirement Fund is not a subsidiary, department or agent of SAG-AFTRA. No portion of SAG-AFTRA's union dues goes to support the AFTRA Retirement Fund's benefits or operational expenses, except for the contributions that SAG-AFTRA makes to provide retirement benefits for its own employees."[2] According to AFTRA Retirement, "SAG-AFTRA [union] and the AFTRA Retirement Fund are separate legal entities, and there are statutory restrictions regarding the sharing of information between the organizations," and "[t]he AFTRA Retirement Fund is a jointly administered fund governed by a Board of Trustees with equal representation from both SAG-AFTRA and contributing industry employers."[3]

15. Defendant SAG-AFTRA Health Plan is a health plan provider that, according to its website, "provides health benefits to tens of thousands of eligible media professionals and their dependents around the globe." SAG-AFTRA Health's principal place of business is located at 3601 West Olive Ave., Suite 200, Burbank, CA 91505. SAG-AFTRA Health also maintains its secondary office in New York.[4] According to Defendant AFTRA Retirement's February 25,

[2] https://aftraretirement.org/Home/learn_about_us/about_us.aspx

[3] https://aftraretirement.org/docs/default-source/default-document-library/registering-with-the-aftra-retirement-fund-your-first-step-toward-benefits4c0d15b1d2446ae9a23dff00001d7895.pdf?sfvrsn=0

[4] https://www.sagaftraplans.org/health/contact

2020 Press Release, the Data Breach "may have impacted the security of personal information of certain current and former plan members of SAG-AFTRA Health Plan."[5]

FACTUAL BACKGROUND

I. AFTRA Retirement Data Breach

16. According to AFTRA Retirement's Press Release, on October 28, 2019, it received an alert of suspicious activity in its environment. AFTRA Retirement launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that an unauthorized individual accessed AFTRA Retirement employees' credit card information and made a small amount of unauthorized purchases using that information.

17. AFTRA Retirement also determined that certain files and folders on its network may have been subject to unauthorized access for periods of time between October 24, 2019 and October 28, 2019, and acknowledged that access to these files could not be ruled out. AFTRA Retirement claims that it then undertook a review of all the files and folders that may have been accessed to determine what sensitive information contained.

18. Although Defendants stated that SAG-AFTRA Health Plan members' data "may have [been] impacted" by the data breach, they have not specified the extent to which Class Members' personal health information ("PHI") may have been compromised.

19. Individuals potentially affected by the Data Breach, including Plaintiff, were first directly notified of the breach by Defendants on February 25, 2020. However, Defendants knew of the Data Breach in October 2019.

[5] https://www.prnewswire.com/news-releases/aftra-retirement-fund---notice-of-data-privacy-event-301011163.html

20. In its materials, brochures, and website, Defendant AFTRA Retirement indicates that it will protect its members' privacy and remain in compliance with statutory privacy requirements. For example, in the June 2019 AFTRA Retirement Plan Summary Plan Description available on its website, AFTRA Retirement states that "[s]ince privacy laws limit how we may share your information, whenever you update your contact information, you must notify the AFTRA Retirement Fund directly — separate from any notifications you send to SAG-AFTRA, the SAG-Producers Pension Plan, the SAG-AFTRA Health Plan and other organizations."[6]

21. Similarly, on the AFTRA Retirement website, Defendant states that "[t]he AFTRA Retirement Fund respects your privacy and is committed to safeguarding your personal information. Our privacy policy is designed to assist you in understanding how we collect and use the personal information you provide to us. When you visit and navigate our site, we will not collect personal information about you unless you provide us that information voluntarily. By "personal information," we mean data that is unique to an individual. We take appropriate physical, electronic, and other security measures to help safeguard personal information from unauthorized access, alteration, or disclosure."[7]

22. Defendant SAG-AFTRA Health also represents itself as being committed to member/patient privacy. For example, according to its website:

> We respect and are committed to protecting your privacy. This Privacy Policy lets you know how and for what purposes we are collecting, processing and using your Personal Information (as defined herein). We pledge that we will take reasonable steps to ensure that your Personal Information and Usage Information (as defined herein) will only be used in ways that are in compliance with this Privacy Policy.[8]

---

[6] https://www.aftraretirement.org/docs/default-source/default-document-library/2019_aftra-retirement-fund_spd_rev-b_new-final_w-nav-links.pdf?sfvrsn=0

[7] https://www.aftraretirement.org/Home/legal/web_privacy_policy.aspx

[8] https://www.sagaftraplans.org/health/privacy

23. SAG-AFTRA Health also affirms its ostensible commitment to privacy and security elsewhere in its online and brochure materials, as well as on certain third party pages it which it redirects. For example, for its privacy policy, SAG-AFTRA Health's 2021 Enrollment Guide redirects to a Via Benefits page stating as follows:

> We have taken certain physical, electronic, contractual and managerial steps to safeguard and secure the personal information we collect. . . .[9]

24. By allowing Class Members' PII and/or PHI to be accessed by cybercriminals, Defendants put all Class Members at risk of identity theft, financial fraud, and other serious harms.

25. Defendants negligently failed to take the necessary precautions required to safeguard and protect the PII and/or PHI of Plaintiff and the other Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

II. Personally Identifiable Information (PII) and Personal Health Information (PHI)

26. PII and PHI are of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful ways.

27. PII and PHI can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone,

---

9 https://documents.viabenefits.com/website/sagaftrahp/1797668_SagAftra_EG_DV_2021_Sample.pdf ("SAG-AFTRA Health Plan has chosen Via Benefits Insurance Services to work with you as you Prepare, Review, and Enroll in new individual Medicare coverage, which will replace your current health plan.") (redirecting to: https://my.viabenefits.com/about/privacy-policy)

or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[10]

28. Given the nature of this breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cyber-criminals in a variety of different ways.

29. Indeed, the cybercriminals who possess Class Members' PII and PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

30. Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years, including during 2019.[11] Indeed, data breaches increased by 17% in 2019 from 2018.[12]

---

[10] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[11] *See e.g.*, Kelly Tyko, *LabCorp data breach exposes information of 7.7 million consumers*, USATODAY (June 4, 2019), https://www.usatoday.com/story/money/2019/06/04/labcorp-data-breach-7-7-million-consumers-affected/1346264001/; Marie C. Baca, *DoorDash data breach affects 4.5 million users*, WASHINGTON POST (Sept. 26, 2019), https://www.washingtonpost.com/technology/2019/09/26/doordash-data-breach-affects-million-users/; Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, NEW YORK TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html; Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN TECH (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/; Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could Be Affected*, CNN TECH (Sept. 8, 2017), https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html; Jim Finkel and David Henry, *Saks, Lord & Taylor Hit By Payment Card Data Breach*, REUTERS (Apr. 3, 2018), https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7; Bill Hutchinson, *87 million Facebook Users To Find Out If Their Personal Data Was Breached*, ABC NEWS (Apr. 9, 2018), https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187.

[12] Meera Jagannathan, *Data breaches soared by 17% in 2019*, MARKETWATCH (Jan. 29, 2020), https://www.marketwatch.com/story/data-breaches-soared-by-17-in-2019-but-theres-some-good-news-too-2020-01-29.

III. Class Members Have Suffered Concrete Injury As A Result Of Defendants' Inadequate Security And The Data Breach It Allowed.

31. Class Members reasonably expected that Defendants would provide adequate security protections for their PII and PHI, and Class Members provided Defendants with sensitive personal information, including their Social Security numbers.

32. The cybercriminals will certainly use the Class Members' PII and PHI, and the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging credit monitoring and protection services.

33. The cybercriminals who obtained the Class Members' PII and PHI may exploit the information they obtained by selling the data in the so-called "dark markets." Having obtained these names, addresses, and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- obtaining medical care;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

34. In addition, if a Class Member's Social Security number is used to create a false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the employee's ability to gain employment or obtain a loan.

35. In addition, as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

36. Moreover, Class Members' health information is uniquely valuable to cyber criminals. The high value of medical records on the dark web has surpassed that of Social Security and credit card numbers. These records can sell for up to $1,000 online, depending on the completeness of the information, according to Experian.[13] Social Security numbers sell for $1, and credit card information goes for up to $110. But Experian reports full medical records can command up to $1,000 because they are full of all the information helpful for committing identity theft: date of birth, place of birth, credit card details, Social Security number, address, and emails.

37. Carbon Black, a cybersecurity company, reports that private health information is worth three times more than traditional personal identifying information due to the fact that health information cannot be changed like a credit card number or a password, rendering victims all the more susceptible to extortion or compromise.[14]

---

[13] Andrew Steger, *What Happens To Stolen Healthcare Data?*, HealthTech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon. *See also* Brian Stack, *Here's How Much Your Personal Information Is Selling For On The Dark Web*, Experian Blog (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[14] Colm Gorey, *Personal health data three times more valuable to hackers than credit card info*, siliconrepublic (June 10, 2019), https://www.siliconrepublic.com/enterprise/personal-health-data-value-cyberattacks.

38. Cybercriminals are very aware of the value these healthcare records possess. These medical records contain an individual's insurance credentials, which is useful for a cybercriminal who cannot qualify or afford medical coverage and needs an expensive medical procedure.[15]

39. Furthermore, both PII and PHI have a long shelf-life because it contains different forms of personal information, can be used in more ways than one and it typically takes longer for an information breach to be detected.[16]

40. As the University of Illinois at Chicago Health Informatics reports: "Financial data can quickly become unusable after being stolen, because people can quickly change their credit card numbers. But medical data are not perishable, which makes them particularly valuable. Some in the medical industry speculate that medical data could grow to rival or surpass financial data in value on the black market[.]"[17]

41. Although patients can have corrected information put in their files, it is difficult to get fraudulent information removed because providers fear medical liability.

42. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[18] Indeed, "[t]he level of risk is

---

[15] Nathan Eddy, *Healthcare data at big risk as hackers innovate and hone their techniques*, HEALTHCAREITNEWS (Sept. 11, 2019), https://www.healthcareitnews.com/news/healthcare-data-big-risk-hackers-innovate-and-hone-their-techniques.

[16] *Id.*

[17] *Why Data Security Is The Biggest Concern in Healthcare*, https://healthinformatics.uic.edu/blog/why-data-security-is-the-biggest-concern-of-health-care/.

[18] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

growing for anyone whose information is stolen in a data breach."[19] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[20] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess Class Members' PII and PHI have not yet used the information but will do so at a later date or re-sell it.

43. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

44. While Defendants represented to the Class Members that there is no evidence that the cybercriminals stole Defendants' data, it is likely that the cybercriminals did and did so undetected. EmiSoft, an award-winning malware-protection software company, states that "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of the investigation."[21]

45. In this case, according to Defendants' own Press Release, cybercriminals had access to Class Members' data between at least October 24 to October 28, 2019 -- a critical amount of time as far as such data breaches are concerned.

---

[19] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[20] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

[21] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

46. Accordingly, that Defendants have not found evidence of stolen data is not an assurance that the data was not stolen. Indeed, the likelihood that the cybercriminals stole the data covertly is significant and concerning.

47. Defendants' poor data security also deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to register and pay Defendants for their service, Plaintiff and other reasonable consumers understood and expected that they were paying for retirement benefit membership, medical services, and data security, when in fact Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

48. Since the Data Breach, Mr. Gilbert has experienced numerous online privacy violations including false payments, bank fraud alerts, and malware.

IV. Breach Is Inadequate To Protect Class Members.

49. Defendants have failed to provide adequate compensation to the Class Members harmed by their negligence. To date, Defendants have only offered Class Members "information on obtaining a free credit report" from Equifax, Experian, or TransUnion. Even if an affected individual enrolls for a credit monitoring service, it will not provide that individual any compensation for the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to signing up for the service. Defendants have not offered Class Members any assistance in dealing with the IRS or state tax agencies. Nor have Defendants offered to reimburse Class Members for any costs incurred as a result of falsely filed tax returns, a likely consequence of the Data Breach.

50. The offered information about credit monitoring services is inadequate to protect the Class Members from the threats they face. It does nothing to protect *against* identity theft.

Instead, it only provides various measures to identify identity theft once it has already been committed.

51. Defendants breached their duty of care in negligently maintaining Plaintiff's PII and PHI. A reasonable person would not have shared PII and PHI with Defendants if they had known that it would not be secure and would be negligently maintained by Defendants.

52. Defendants have a duty to protect their patrons and patrons' property.

53. Defendants should have known -- and perhaps had actual knowledge -- that data breaches including breaches impacting health data, were on the rise and medical institutions were lucrative or likely targets of cybercriminals looking to steal PII and PHI. As mentioned above, data breaches such as the one that occurred at Defendants' network dominated headlines and should have been known to any and all medical institutions which take reasonable precaution to secure the data it maintains. Defendants owed an affirmative duty to exercise reasonable or ordinary care for the safety of the PII and PHI of their members, especially given that a data breach was foreseeable. Defendants had reason to anticipate an assault on its computer system as a medical institution warehousing and storing valuable and private information of its patients.

54. Defendants voluntarily undertook the act of maintaining and storing Plaintiff's PII and PHI and as such, the law required Defendants to do so with ordinary or reasonable care. Defendants breached that duty when they failed to implement safety and security enough to protect from the data breach that it should have anticipated.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of himself and all individuals whose PII or PHI was compromised as a result of the AFTRA Retirement Fund or SAG-AFTRA Data Breach (the "Nationwide Class").

56. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a California Sub-class under the laws of the State of California, defined as follows:

> "All persons residing in California and non-residents, whose PII or PHI was compromised as a result of the AFTRA Retirement's Data Breach."

57. Plaintiff reserves the right to amend the above definitions, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

58. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise controls or controlled; and any legal representative, predecessor, successor, or assignee of Defendants.

59. Plaintiff believes that the proposed Class and Sub-class as described above consist of over 57,000 members and can be identified through Defendants' records, though the exact number and identities of the Class Members are currently unknown. The Class and Sub-class are therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

60. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendants had a duty to protect the Class Members' PII and PHI;

b. Whether Defendants breached their duty to protect the Class Members' PII and PHI;

c. Whether Defendants disclosed Class Members' PII and PHI;

d. Whether Defendants timely, accurately, and adequately informed Class Members that their PII and PHI had been compromised;

e. Whether Defendants' conduct was negligent; and

f. Whether Plaintiff and Class Members are entitled to damages.

61. The claims asserted by Plaintiff are typical of the claims of the members of the Class he seeks to represent because, among other things, Plaintiff and Class Members sustained similar injuries as a result of Defendants' uniform wrongful conduct; Defendants owed the same duty to each Class Member; and Class Members' legal claims arise from the same conduct by Defendants.

62. Plaintiff will fairly and adequately protect the interests of the proposed Class. Plaintiff's interests do not conflict with the Class Members' interests. Plaintiff has retained class counsel experienced in class action litigation to prosecute this case on behalf of the Class.

63. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendants.

64. Defendants have acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

65. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the thousands and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class Members to prosecute their claims individually. Trial of Plaintiff's and the Class Members' claims is manageable. Unless the Class is certified,

Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

66. The prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendants.

67. Defendants' wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

68. Defendants' systemic policies and practices also make injunctive relief for the Class appropriate.

69. Absent a class action, Defendants will retain the benefits of their wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiff and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf Of Plaintiff And The Nationwide Class)

70. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

71. Plaintiff brings this claim on behalf of himself and the Class.

72. The Class Members are individuals who provided certain PII and PHI including their addresses, dates of birth, driver's license numbers (or other form of state-issued identification), financial information, health information related to treatment at SAG-AFTRA Health or referring providers, health insurance numbers, Social Security numbers, and email addresses to Defendants as a necessary condition of Defendants providing its medical or clinical services to the Class Members.

73. Defendants had full knowledge of the sensitivity of the PII and PHI and the types

of harm that Class Members could and would suffer if the PII or PHI were wrongfully disclosed. Defendants had a duty to each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Class Members were the foreseeable victims of any inadequate safety and security practices. Class Members had no ability to protect their data that was in Defendants' possession.

74. Defendants had a duty to Plaintiff and Class Members to safeguard and protect their PII and PHI. Defendants' duty to the Plaintiff and other Class Members included, *inter alia*, establishing processes and procedures using reasonable and industry-standard care to protect the PII and PHI from wrongful disclosure and training employees who had access to the PII and PHI as to those processes and procedures.

75. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII and PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

76. Defendants had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Class Members' PII and PHI data.

77. Defendants breached their duty of care by failing to adequately secure, safeguard, and protect the Class Members' PII and PHI from theft, collection, and misuse by third parties. Defendants negligently stored and/or maintained its systems.

78. Further, Defendants, by and through their above negligent actions and/or inaction, further breached its duties to Class Members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Class Members' PII and PHI within their possession, custody, and control.

79. Defendants admitted that Class Members' PII and PHI were wrongfully exposed as a result of the Data Breach.

80. Class Members have suffered harm as a result of Defendants' negligence, including financial injury. These victims' loss of control over the compromised PII and PHI subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from use of the compromised information.

81. It was reasonably foreseeable -- in that Defendants knew or should have known -- that their failure to exercise reasonable care in safeguarding and protecting Class Members' PII and PHI would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII or PHI or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

82. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Class Members, the PHI would not have been compromised.

83. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Class Members' PII or PHI, the Class Members have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm -- for which they are entitled to compensation. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence and/or negligent misrepresentation.

84. Class Members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Breach Of Express Contract
(On Behalf Of Plaintiff And The Nationwide Class)

85. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

86. Plaintiff brings this claim on behalf of himself and the Class.

87. Plaintiff and Class Members entered into written agreements with Defendants as part of the retirement fund or health plan services and data security Defendants provided to Class Members. The agreements involved a mutual exchange of consideration whereby Defendants provided retirement fund or health plan services for Class Members in exchange for payment from Class Members and/or Class Members' insurance carriers or SAG-AFTRA union dues or government programs remitting payment on Class Members' behalf.

88. Defendants' failure to protect Class Members' PII and PHI constitutes a material breach of the terms of the agreement by Defendants.

89. As a direct and proximate result of Defendants' breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

90. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully request this Court award all relevant damages for Defendants' breach of express contract.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf Of Plaintiff And The Nationwide Class)

91. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

92. Plaintiff brings this claim on behalf of himself and the Class.

93. Class Members provided their PII and PHI to Defendants in order to utilize Defendants' retirement fund and health plan services.

94. Class Members provided various forms of PII and PHI to Defendants as a condition

precedent to the use of Defendants' services.

95. Understanding the sensitive nature of PII and PHI, Defendants implicitly promised Class Members that they would take adequate measures to protect their PHI.

96. Indeed, a material term of this contract is a covenant by Defendants that they will take reasonable efforts to safeguard Class Members' PII and PHI.

97. Class Members relied upon this covenant and would not have consented to the disclosure of their PII and PHI without assurances that it would be properly safeguarded. Moreover, the covenant to adequately safeguard Class Members' PII and PHI is an implied term, to the extent it is not an express term.

98. Class Members fulfilled their obligations under the contract by providing their PII and PHI to Defendants.

99. Defendants, however, failed to safeguard and protect the Class Members' PII and PHI. Defendants' breach of their obligations under the contract between the parties directly caused Class Members to suffer injuries.

100. As the direct and proximate result of Defendants' breach of the contract between Defendants and the Class Members, Class Members have been and continue to be damaged as described above.

101. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully requests this Court award all relevant damages for Defendants' breach of contract.

FOURTH CAUSE OF ACTION
Unjust Enrichment/Quasi-Contract
(On Behalf Of Plaintiff And The Nationwide Class)

102. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

103. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased services from Defendants and provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and should have been entitled to have Defendants protect their PII and PHI with adequate data security.

104. Defendants knew that Plaintiff and Class Members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendants profited from Plaintiffs' purchases and used Plaintiffs' and Class members' PII and PHI for business purposes.

105. Defendants failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' private information provided. Defendants also benefits because they did not spend that portion of the moneys paid by Plaintiff and Class Members that should have been spent on data security.

106. Defendants acquired the PII and PHI through inequitable means as they failed to disclose the inadequate security practices previously alleged.

107. If Plaintiff and Class Members knew that Defendants would not secure their PII and PHI using adequate security, they would not have sought retirement fund and health plan services from Defendants.

108. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on them.

109. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid.

FIFTH CAUSE OF ACTION
Violations of New York Consumer Law for Deceptive Acts and Practices N.Y. Gen. Bus. Law § 349
(On Behalf Of Plaintiff And The Nationwide Class)

110. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

111. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

112. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

113. Defendants stored Plaintiff's and the Class Members' PII and PHI in Defendants' electronic and consumer information databases. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and the Class members' PII and PHI secure and prevented the potential loss or misuse of Plaintiffs' and the Class members' PII and PHI. Defendants did not disclose to Plaintiffs and the Class members that their data systems were not secure.

114. Defendants have engaged in repeated and persistent deceptive acts and practices, including but not limited to:

a. Misrepresenting to consumers, expressly and by implication, that it provided reasonable safeguards to protect consumers' personal information from loss, misuse, and unauthorized access and disclosure;

b. Misrepresenting to consumers, expressly and by implication, the manner in which

their accounts were compromised;

c. Misrepresenting to consumers, expressly and by implication, that their accounts had not been accessed without authorization;

d. Misrepresenting to consumers, expressly and by implication, its vendor's findings regarding third parties' attempts to access the consumers' accounts; and

e. Misrepresenting to consumers, expressly and by implication, the success of third parties' attempts to access the consumers' accounts.

115. Plaintiff and the Class never would have provided their sensitive and personal PII and PHI if they had been told or knew that Defendants failed to maintain sufficient security to keep such PII and PHI from being hacked and taken by others, and that Defendants failed to maintain the information in encrypted form.

116. Defendants violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendants' many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and the Class Members' PII and PHI.

117. Plaintiff and the Class paid a price premium for Defendants' services, expecting that their critical PII and PHI would be kept secured.

118. Defendants also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class Members of the Security Breach. If Defendants had complied with these legal requirements, Plaintiff and the other Class Members would not have suffered the damages related to the Security Breach.

119. Defendants actively and knowingly misrepresented or omitted disclosure of

material information to Plaintiff and the Class at the time they provided such information, that Defendants did not have sufficient security or mechanisms to protect their PII and PHI.

120. Defendants failed to give timely warnings and notices regarding the defects and problems with their system(s) of security systems that they maintained to protect Plaintiff's and the Class Members' PII and PHI. Defendants possessed prior knowledge of the defects -- including potential hacks from cybercriminals -- in their IT systems and failed to address the same or to give timely warnings that there had been a Data Breach.

121. Defendants' intentional concealments were designed to deceive current and prospective members/customers into believing that their critical PII and PHI was secure. By concealing its actual deficient data security systems and procedures and delaying notification after the Data Breach, (artificially inflating prices and maximizing profits), Defendants deprived consumers from being able to make informed purchasing decisions.

122. Defendants' wrongful conduct caused Plaintiff and the Class to suffer consumer-related injuries by causing them to incur substantial expense to protect from misuse of their PII and PHI by third parties and placing the Plaintiff and the Class at serious risk for monetary damages.

123. As a direct and proximate result of Defendants' unlawful deceptive acts and practices, Plaintiff and Class Members subscribed to or remained with Defendants while their data security mechanisms were deficient and after the Data Breach had occurred. They suffered and continue to suffer an ascertainable loss of monies based on the wrongful violations of their PII, PHI, and privacy. By reason of the foregoing, Defendants are liable to Plaintiff and Class Members for trebled compensatory damages, attorneys' fees, and the costs of this suit.

124. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class

Members suffered damages as alleged above.

125. In addition to or in lieu of actual damages, because of the injury, Plaintiff and Class Members seek statutory damages for each injury and violation which has occurred.

SIXTH CAUSE OF ACTION
Violation of New York's Data Breach Laws – Delayed Notification, N.Y. Gen. Bus. Law § 899-aa
(On Behalf Of Plaintiff And The Nationwide Class)

126. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

127. Section 899-aa(3) of NYGBL requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

128. Section 899(5) of NYGBL states:

> The notice required by this section shall be directly provided to the affected persons by one of the following methods:
>
> (a) written notice;
>
> (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
>
> (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
>
> (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the

following:

> (1) e-mail notice when such business has an e-mail address for the subject persons;
> (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
> (3) notification to major statewide media.

129. The Security Breach described in this Complaint constitutes a "breach of the security system" of Defendants.

130. As alleged above, Defendants unreasonably delayed informing Plaintiff and Class Members about the Security Breach, affecting the confidential and non-public Private Information of Plaintiff and the Nationwide Class after Defendants knew the Security Breach had occurred.

131. GBL § 899-aa requires that businesses disclose, in the most expedient time possible and without unreasonable delay, a breach of security to all New York State residents whose private information was, or is reasonably believed to have been, acquired without valid authorization.

132. Furthermore, GBL § 899-aa requires that, in the event New York State residents are required to be notified of a breach, businesses also notify the OAG, the New York Department of State, and the New York Division of State Police.

133. Defendants failed to disclose to Plaintiff and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when Defendants knew or reasonably believed such information had been compromised.

134. Defendants' ongoing business interests gave Defendants incentive to conceal the Security Breach from the public to ensure continued revenue.

135. Upon information and belief, no law enforcement agency instructed Defendants that notification to the Plaintiff and Nationwide Class would impede Defendants' investigation.

136. As a result of Defendants' violation of New York law, Plaintiff and the Nationwide

Class were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, including retaining credit and identity monitoring services, securing identity theft protection, or requesting a credit freeze.

137. As a result of Defendants' violation of New York law, Plaintiff and the Nationwide Class have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

138. Plaintiff and Class Members seek all remedies available under New York law, including, but not limited to damages the Plaintiff and the New York Subclass suffered as alleged above, as well as equitable relief

SEVENTH CAUSE OF ACTION
Violation of California Consumer Legal Remedies Act ("CLRA"),
Cal. Civ. Code § 1750, *et seq*.
(On Behalf Of Plaintiff And The California Subclass)

139. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

140. Defendants' implied and express representations that it would adequately safeguard Class Members' PHI are false and deceptive because reasonable consumers understand and expect that Defendants would provide adequate data security, and they constitute representations as to characteristics, uses, or benefits of services that such characteristics, uses, or benefits did not actually have.

141. These violations have caused financial injury to the Class Members.

142. Plaintiff and other Class Members bring this action under the Consumer Protection Act to enjoin further violations, to recover actual damages, and to recover costs of this action, including reasonable attorneys' fees.

143. Plaintiff and the other members of the California Sub-Class are consumers who

purchased, directly or indirectly, services from Defendants for personal retirement and health plan services.

144. Defendants engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiff and the other members residing in California.

145. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' acts, practices and omissions were done in the course of their business of marketing, offering for sale, and selling goods and services in the United States, including in the state of California.

146. Defendants' conduct, as alleged in this Complaint, including without limitation their failure to maintain adequate computer systems and data security practices to safeguard customers' PII and PHI, Defendants' failure to disclose the material fact that their computer systems and data security practices, was inadequate to safeguard Class Members' PII and PHI from theft.

147. As a result of Defendants' deceptive conduct, Plaintiff and members of the Class Members have been injured by the Data Breach. Plaintiff and members of Class Members are entitled to, *inter alia*, injunctive relief and other such relief the Court deems appropriate, just, and equitable, to be determined at trial.

148. Plaintiff has provided Defendants with notice of its violations of the CLRA pursuant to Cal. Civ. Code § 1782(a). The notice, attached hereto as Exhibit A, has been transmitted to Defendants prior to the filing of this complaint. Plaintiff reserves the right to, upon the expiration of thirty days from the date of mailing the notice, amend this complaint to include a request for damages under the CLRA.

149. Accepting Plaintiff and Class Members' most sensitive PII and PHI without providing adequate safeguards constitutes an unconscionable trade practice. Because Defendants did not provide adequate data security, Plaintiff and Class Members were unable to receive a material benefit of their transactions, and the transactions were excessively one-sided.

EIGHTH CAUSE OF ACTION
Violation Of California's Unfair Competition Law ("UCL") California Business & Professions Code § 17200, *et seq.*
(On Behalf Of Plaintiff And The California Subclass)

150. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

151. California Business & Professions Code § 17200, et seq., the UCL, prohibits "any unlawful, unfair or fraudulent business act or practice."

152. At all relevant times, Defendant has maintained substantial operations in, regularly conducted business throughout, and engaged in the conduct described herein within the State of California.

153. Plaintiff and the other members of the California Sub-Class are consumers who purchased, directly or indirectly, services from Defendants for personal retirement and health plan services.

154. Defendants engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiff and the other members residing in California.

155. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' acts, practices and omissions were done in the course of their business of marketing, offering for sale, and selling goods and services in the United States, including in the state of California.

156. Defendants, in connection with their data security policies and the Data Breach, have engaged in unfair, unlawful, and fraudulent business acts and practices in violation of the UCL in that: (1) Defendant's conduct is immoral, unethical, oppressive, unconscionable, and substantially harmful to Plaintiff and members of the Class; (2) any justification for Defendant's conduct would be outweighed by the gravity of the injury to Plaintiff and members of the Class; (3) Defendant's conduct violates the common law and the CLRA; and (4) Defendant's conduct deceived and defrauded Plaintiff and members of the Class.

157. Defendants' unfair, unlawful, and fraudulent business practices were likely to deceive a reasonable consumer. Plaintiff and Class Members used Defendants' services under the expectation that their PII and PHI would be secured.

158. Defendants' conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices in violation of The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. And Prof. Code, § 17200, *et seq*.

159. As a result of Defendants' deceptive conduct, Plaintiff and members of the Class Members have been injured by the Data Breach.

160. Defendants' conduct is or may well be continuing and ongoing. Accordingly, Plaintiff and members of the Class are entitled to injunctive relief to prohibit or correct such ongoing acts of unfair competition, in addition to obtaining equitable monetary relief.

NINTH CAUSE OF ACTION
Violation Of The California Customer Records Act, § 1798 *et seq*.
(On Behalf Of Plaintiff And The California Subclass)

161. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

162. The Data Breach described above constituted a "breach of the security system" of Defendants, within the meaning of Section 1798.82 (g) of the California Civil Code.

163. The information lost in the Data Breach constituted "personal information" within the meaning of Section 1798.80(e) of the California Civil Code.

164. 144. Under Cal Civ. Code § 1798.81.5(d)(1)(A)(i-iv), "personal information," as described in Cal Civ. Code § 1798.81.5(b), means the following:

> (A) [a]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number or California identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

165. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

166. Defendants unreasonably delayed informing anyone about the breach of security of Plaintiff and the Class Members' confidential and non-public information after Defendants knew the Data Breach had occurred.

167. Defendants failed to disclose to Plaintiff and Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when they knew or reasonably believed such information had been compromised.

168. By failing to promptly notify all affected members that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Defendants violated Civil Code section 1798.82 of the same title. Defendants' failure to timely notify employees of the breach has caused class members damages who have had to buy identity protection services or take other measures to remediate the breach caused by

Defendants' negligence.

169. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiff and Class Members would impede investigation.

170. As a result of Defendant's violation of Cal. Civ. Code § 1798.80 *et seq.*, Plaintiff and Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

171. Plaintiff, individually and on behalf of the Class, seeks all remedies available under Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California Sub-Class as alleged above; (b) statutory damages for Defendants' willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief. Additionally, as a result of Defendants' violation of Civil Code sections 1798.81.5, and 1798.82, Plaintiff and Class Members have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

172. Plaintiff, individually and on behalf of the Class, also seeks reasonable attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).

173. Because Defendants violated Cal. Civ. Code Sections 1798.81.5 and 1798.82, and continues to violate Cal. Civ. Code Section 1798.82, Plaintiff may seek an injunction pursuant to Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Specifically, Plaintiff seeks injunctive relief as follows -- Defendants must implement and maintain adequate and reasonable data security measures and abide by the California Data Breach laws, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems periodically, and ordering Defendants to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training their security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of Defendants' data security measures are compromised, hackers cannot gain access to other areas of Defendants' systems;

f. deleting, in a reasonable and secure manner, Personal Information not necessary for Defendants' provisions of services;

g. conducting regular database scanning and security checks;

h. issue security breach notifications to California Residents which abide by the requirements established under Cal. Civ. Code Section 1798.82(d);

i. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs

and what appropriate actions are proper in response to a breach; and

j. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves and assisting with said steps by providing credit monitoring services.

TENTH CAUSE OF ACTION
Violation Of The Confidentiality of Medical Information Act Under California Civil Code § 56, *et seq.*
(On Behalf Of Plaintiff And The California Subclass)

174. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

175. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

176. At all relevant times, Defendant SAG-AFTRA Health was a health care provider because it had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code 6 § 56.06(a).

177. At all relevant times. Defendant SAG-AFTRA Health collected, stored, managed, and transmitted Plaintiff's and Class Members' PII/PHI.

178. The CMIA requires Defendant SAG-AFTRA Health to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and maintained by them. Specifically, California Civil Code § 56.10(a) prohibits Defendant from

disclosing Plaintiff's and Class Members' PHI without first obtaining their authorization to do so.

179. Section 56.11 of the California Civil Code specifies the manner in which authorization must be obtained before PHI is released. Defendants, however, failed to obtain any authorization - let alone, proper authorization - from Plaintiff and Class Members before releasing and disclosing their PHI. Defendant also failed to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PHI as required by California law. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' PHI was disclosed. By disclosing Plaintiff's and Class Members' PHI without their written authorization. Defendant SAG-AFTRA Health violated California Civil Code § 56, *et seq.*, and their legal duty to protect the confidentiality of such information.

180. SAG-AFTRA Health also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential PHI. As a direct and proximate result of SAG-AFTRA Health's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' confidential PHI was viewed, released and disclosed without their authorization by unauthorized persons.

181. As a direct and proximate result of SAG-AFTRA Health's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members also are entitled to (i) injunctive relief, (ii) punitive damages of up to $3,000 per Plaintiff and each Class Member, and (iii) attorneys' fees, litigation expenses and court costs under California Civil Code

§ 56.35.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class, respectfully requests that the Court grant relief against Defendants as follows:

A. For an Order certifying that this action may be prosecuted as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) and requiring notice thereto to be paid by Defendants;

B. Appointing Plaintiff and his counsel to represent the Class;

C. For appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing PII and PHI, and to provide identity theft monitoring for an additional five years;

D. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

E. For actual, compensatory, statutory, and general damages in an amount to be determined, as allowable by law;

F. For reimbursement, restitution, and disgorgement on certain causes of action;

G. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

H. For costs of the proceedings herein;

I. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

J. For an Order awarding Plaintiff and the Class reasonable attorney's fees and expenses for the costs of this suit;

K. Trial by jury; and

L. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Dated: December 22, 2020
White Plains, New York

By: s/ Todd S. Garber

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
Todd S. Garber
D. Greg Blankinship
Jeremiah Frei-Pearson
Sami Ahmad
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561
tgarber@fbfglaw.com
gblankinship@fbfglaw.com
jfrei-pearson@fbfglaw.com
sahmad@fbfglaw.com

KELLER LENKNER LLC
Warren Postman (*Pro Hac Vice* application forthcoming)
1300 I Street, N.W., Suite 400E
Washington, D.C. 20005
Tel: (312) 948-8463
wdp@kellerlenkner.com

Attorneys for Plaintiff and the Putative Class